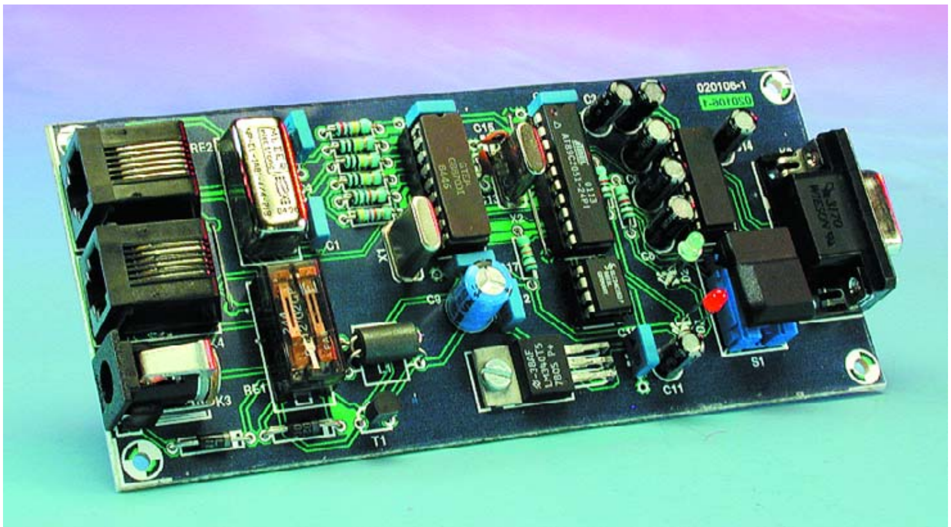
Programmable Dial-Out Blocking Device

barring premium rate numbers

Design by C. Lercher

Premium rate numbers (in the UK, generally those starting with 09) are often used as a way of extracting payments from telephone users and Internet surfers. This is however illegal if it is done covertly without the knowledge of the user. The circuit described here blocks such numbers and cannot be defeated.



Despite the best endeavours of consumer protection organisations there is still much abuse of premium rate telephone numbers. In particular, it can happen that while surfing the Internet, unbeknown to the user, a new dialler program is downloaded which terminates the call in progress and dials out again on an expensive premium rate number. Unfortunately dialler guard programs are no defence against such underhand activity, since as soon as some new piece of protection software appears it only takes the hackers a short while to develop a way to get around its security. It is of course possible to arrange for your telephone provider to bar premium rate numbers, but not generally if a carrier selection prefix is used — which if often the case with such diallers. An external device is called for, which cannot be hacked into, but which nevertheless can be updated with new numbers as required.

What are premium rate numbers?

Variable or fixed tariff premium rate numbers appear in a special separate section on the telephone bill. The charge for such calls can vary from a few pence to pounds per call or per minute. This is all perfectly legal, and provides a straightforward way to charge for services such as directory enquiries or helplines. As is so often the case, however, there is a darker side: when you use a dialler program which drops your

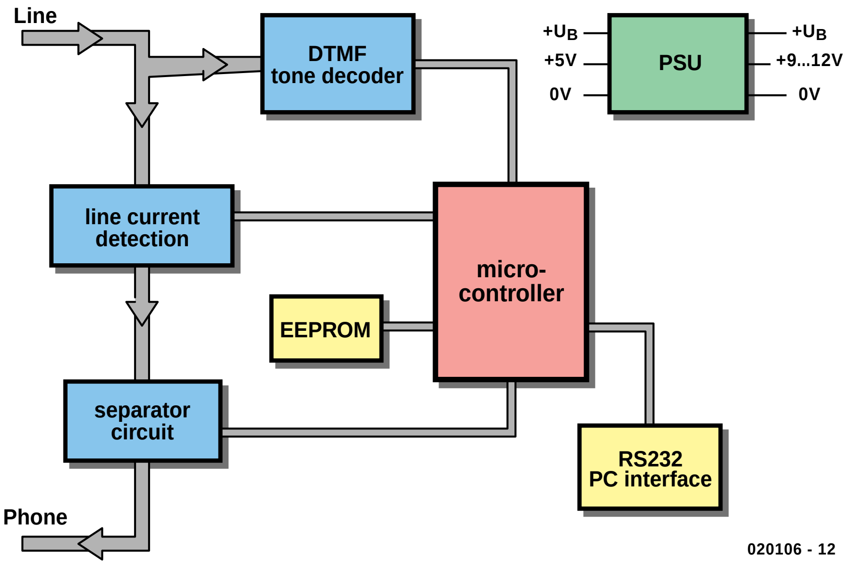


Figure 1. Block diagram of the Programmable Dial-Out Blocking Device.

modem or ISDN Internet connection and, without your knowledge, re-establishes it over an expensive premium rate number.

This Programmable Dial-out Blocking Device prevents such connections being made by barring up to ten freely-programmable numbers or number prefixes. Thus, for example, not only can 09-prefix numbers can be blocked, so can others: to allow only local calls, to bar international calls, to prevent carrier selection prefixes, and so on.

Between linebox and modem

A block diagram of the device is shown in **Figure 1**. Like an answering machine, it is connected in series with the telephone line and becomes active when the line is in use, i.e. when the receiver is picked up. It is capable of recognising the sequence of DTMF tones that correspond to a number to be barred and then breaking the connection, thus dropping the call.

To do this, two functional blocks are connected in series with the telephone line, namely a loop current monitor and a line interrupter. These two blocks are connected to a microcontroller, along with a DTMF tone decoder and an external I^2C EEPROM in which the numbers to be blocked are stored. The device is programmed over an RS232 interface, which employs a MAX 232, and therefore uses standard symmetrical voltage levels. A mains power supply delivering a stable +5 V completes the circuit.

The circuit is designed so that in the event of a power cut the telephone line can be used freely. This is hardly a disadvantage — one can after all always simply pull out the plug in order to dial a barred number — but is rather a safety feature: if there is a power cut as a result of a fire, it will always still be possible to call the fire brigade!

When a piece of terminal apparatus such as an analogue modem or fax machine goes off-hook in order to make a call, the series-wired line sensing relay is energised. This is just an ordinary relay, except that its coil has an extremely low resistance. This is so that we do not insert too much additional resistance into the telephone circuit. Line sensing relays typically have a resistance of less than 10 Ω. The current through the terminal apparatus and the line sensing relay is in the region of 20 mA, which corresponds to a voltage drop of around 200 mV. When this current flows, a tiny reed contact closes in the relay: this can even be seen in the symbol shown in **Figure 2**. The relay is polarity sensitive: this means that the direction of current flow in the coils is important. If opposing currents flow in the two coils, the magnetic fields cancel one another out and the reed contact does not close.

When the line sensing relay detects a connection, it sends a signal to the microcontroller which then starts to monitor the output of the DTMF decoder.

The DTMF tone pairs are AC-coupled from the telephone line via coupling capacitors C1 and C4. The IN+, IN- and GS pins of the MT8870 are connected to an internal operational amplifier, whose gain can be set using R4. R6 and R7 form a high-impedance connection to V_{ref}. According to the datasheet, a voltage of $V_{dd}/2$, or around 2.5 V, is present on this pin. The R5-C2 RC combination effectively measures the length of the DTMF tones, and, if the length is correct, a pulse is generated on STD. The falling edge indicates that a tone has been decoded and that a valid decoded result is available on the data output pins.

The microcontroller

The main control tasks are carried out by an Atmel 89C2051 microcontroller. On reset the microcontroller first checks wither pin P3.2 is low. If this is the case, the system establishes a terminal connection with a remote PC over the RS232 interface, as the DTR input signal (pin 4 on connector K2) is asserted. Since the CD and DSR signals (pins 1 and 6 respectively) are connected to DTR, the computer (or rather a terminal program running on it) will be able to establish communication.

A serial 256 by 8 bit EEPROM memory is connected to the microcontroller. The microcontroller drives the EEPROM via an I^2C two-wire bus.

Two LEDs are also connected to the microcontroller. The red LED D3 lights to indicate when the line is busy, and goes out automatically when the first DTMF tone is recognised. The green LED D3 indicates when the circuit is ready for operation. It lights continuously except when the unit has been disabled for the next call by pressing button S1, or when a connection with the host computer has

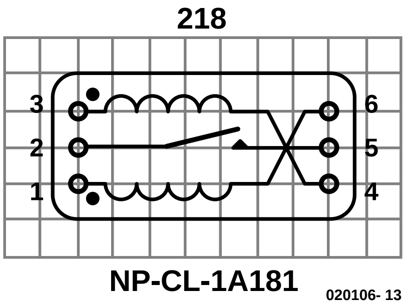


Figure 2. Line sensing relay pinout.

been established.

The device uses two six-way RJ11 sockets. RJ12 sockets can also be used, as long as the pinout is correct. Eight-way RJ45 data/ISDN sockets are sometimes also found on analogue connections, and these can also be used, although this does not conform to ETSI standards.

The line socket can be connected either directly to the master socket or in line with the modem's cable. The telephone socket is then connected to the telephone or modem respectively. Information on the pinout of RJ connectors and lineboxes can be found on the Internet, for example at www.gbnet.net/net/uk-telecom/p3-1.html.

The connection to the host computer is set up as follows:

- connect the RS232 cable (not a null-modem cable)
- start the terminal program
- briefly interrupt the power to the circuit, in order to reset it

What happens now, if the modem or other terminal device goes off-hook? Because the line sensing relay coils form a series circuit with the terminal device via K1, the reed contact in the line sensing relay will close when the line becomes busy. This information is communicated to the microcontroller in the form of a falling edge on input P1.7. The line becoming busy is also indicated by LED D3. The microcontroller has internal pull-ups, and so external resistors are not required. Contact bounce is eliminated in software.

High nibble of address	Low nibble of address																barred number
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0	30	31	39	30	0D												0190
1	30	31	39	33	0D												0193
2	30	39	30	30	0D												0900
3	30	31	30	78	78	30	31	39	0D								010xx0190
4	30	31	30	78	78	30	31	39	33	0D							010xx0900
5	30	31	30	78	78	30	39	30	30	0D							010xx0193
6	30	31	30	78	78	78	30	31	39	30	0D						010xxx0190
7	30	31	30	78	78	78	30	31	39	30	0D						010xxx0900
8	30	31	30	78	78	78	30	39	30	30	0D						010xxx0193
9	30	30	0D														00

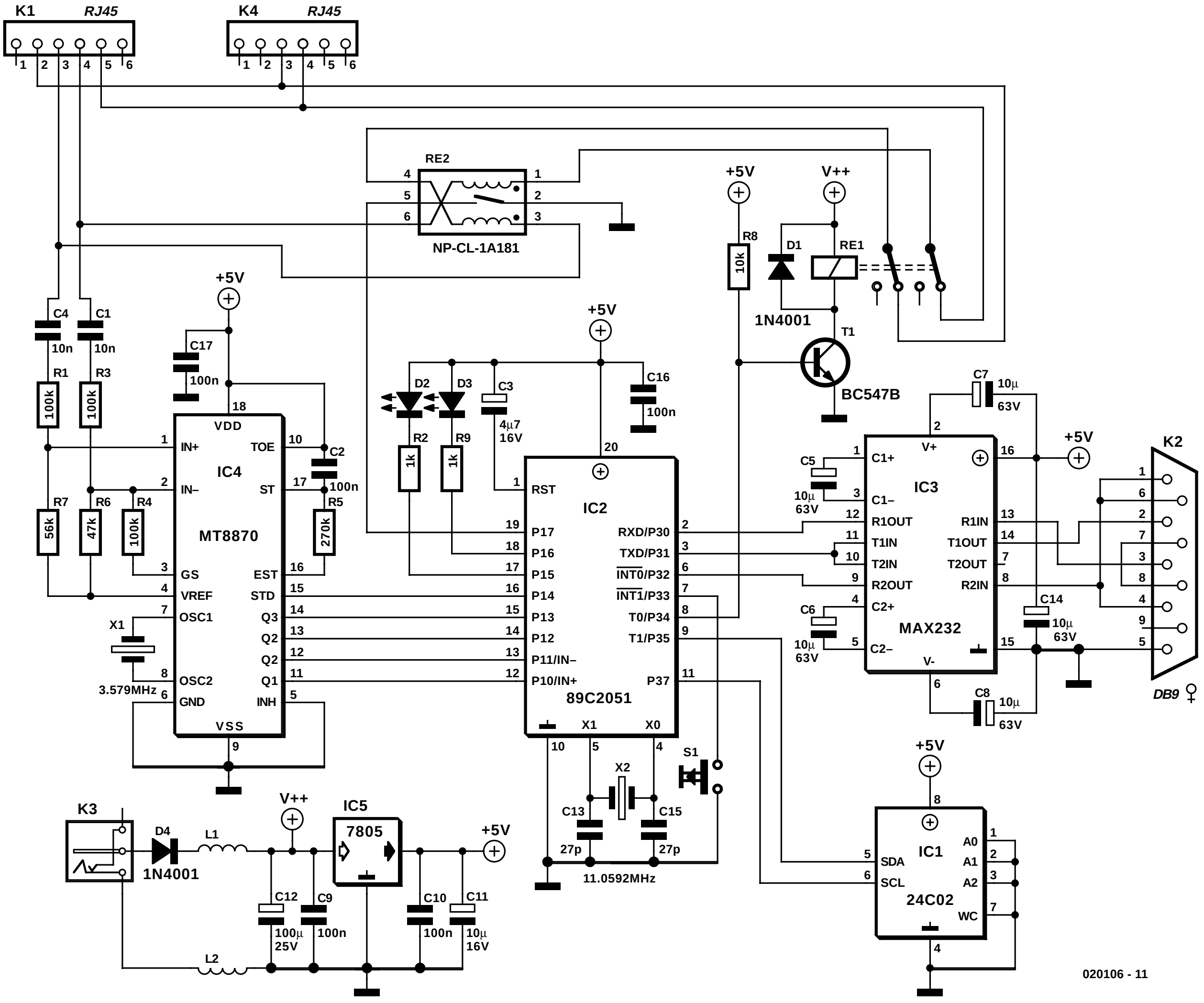


Figure 3. Detailed circuit diagram.

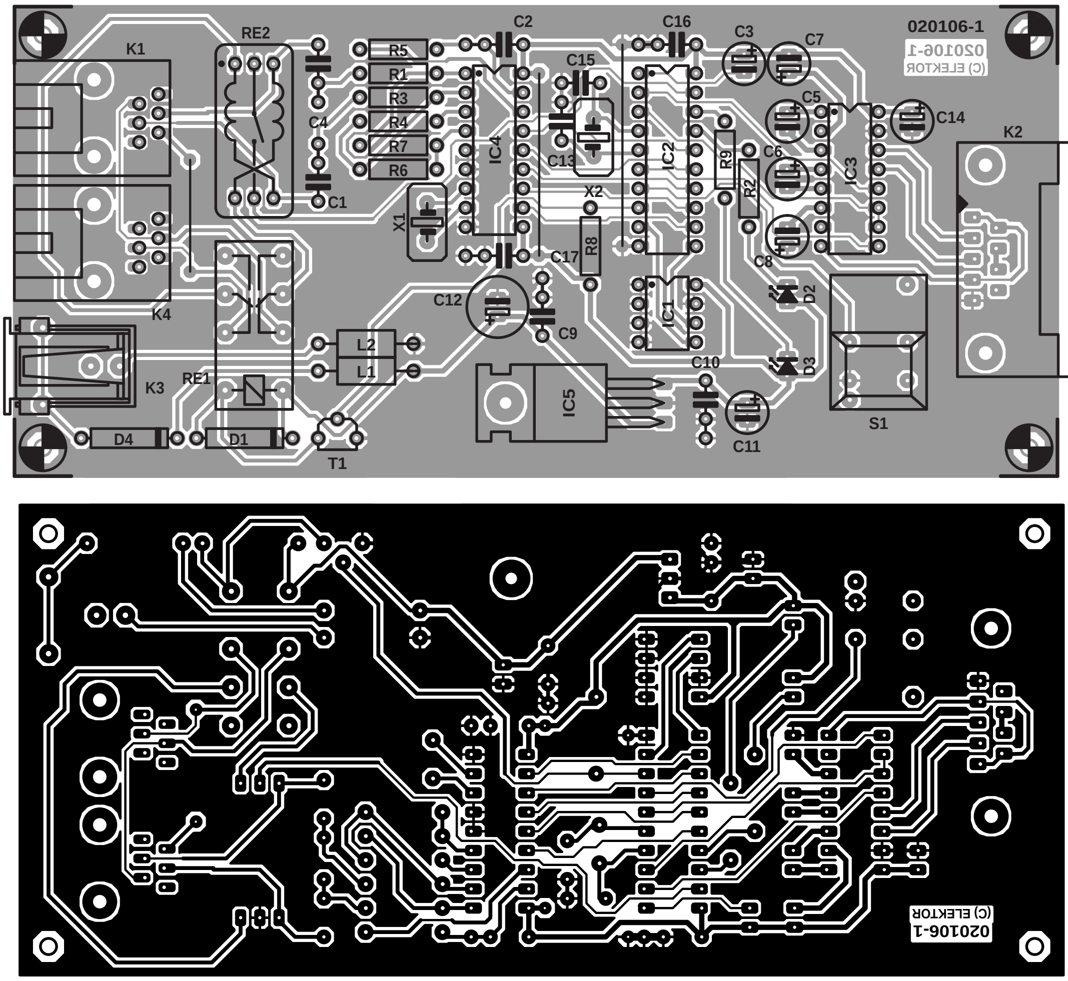


Figure 4. The single-sided printed circuit board (available ready-made).

Next, a number is dialled. Rising edges on input P1.4 indicate to the microcontroller when a new DTMF tone has been recognised. As soon as the signal goes low, the microcontroller can read the data as a 4-bit value on pins P1.0 to P1.3. This value can now be compared with the first storage location in the number table. The storage format of barred numbers in the EEPROM is illustrated in the table. At this point the microcontroller has detected a valid tone and converted the code into an ASCII value. A pointer into the table is used which starts in column zero and compares each entry with the decoded DTMF tone. For example, suppose the tone corresponds to the digit zero (30_{hex}). This matches in rows 0, 1, 2 and 9, and so in each of those rows the column pointer can be advanced to column 1. For all the other rows the column pointer is set to the value FF_{hex} to indicate that the row in question is no longer in consideration. Suppose the next

COMPONENTS LIST

Resistors:

R1,R3,R4 = 100kΩ
R2,R9 = 1kΩ
R5 = 270kΩ
R6 = 47kΩ
R7 = 56kΩ
R8 = 10kΩ

Capacitors:

C1,C4 = 10nF
C2,C9,C10,C16,C17 = 100nF
C3 = 4µF7 16V radial
C5-C8,C11,C14 = 10µF 63V radial
C12 = 100µF 25V radial
C13,C15 = 27pF

Inductors:

L1,L2 = 2-hole ferrite core, 2 x 2 turns ECW

Semiconductors:

D1,D4 = 1N4001
D2 = LED, green, high efficiency
D3 = LED, red, high efficiency
T1 = BC547B
IC1 = EEPROM, 24C02 or larger, in DIL8 case
IC2 = AT89C2051, programmed, order code **020106-41**
IC3 = MAX232CP
IC4 = MT8870 or KT3170
IC5 = 7805

Miscellaneous:

K1,K4 = 6-way RJ45- or RJ11 socket, PCB mount
K2 = 9-way sub-D socket (female), angled pins, PCB mount
K3 = mains adaptor socket
S1 = pushbutton, 1 make contact
X1 = 3.579545MHz (NTSC) quartz crystal (32pF parallel resonance)
Re1 = 12V relay, 2 changeover contacts, Fujitsu D012-02CP or Siemens V23042-A2003-B101
X2 = 11.0592MHz quartz crystal (32pF parallel resonance)
Re2 = NP-CL-1A181-4/4-218 (Meder/Finder/Omron) supplied by ELV (*www.elv.de*)
PCB, order code **020106-1**
Disk, project software, order code **020106-11**

digit is 9 (39_{hex}). This matches only in row 2; now for rows 0, 1 and 9 the column pointer is also set to the flag value FF_{hex}.

The wildcards indicated by ‘x’ (78_{hex}) represent blocks of digits. This function is used to allow the various network access numbers used for carrier selection to be recognised. The particular access code used does not matter; what is important is whether an expensive 09-prefix number follows or not, because this is what must be detected correctly to ensure that the connection can be broken. A table entry of $0D_{hex}$ corresponds to an ‘enter’ command and causes the call to be dropped.

Construction and test

Start as usual by populating the printed circuit board (**Figure 4**) with the smaller components such as resistors, diodes and wire links. Then fit the IC sockets, relays, connectors and capacitors.

With just voltage regulator IC5 fitted, carry out an initial test by applying 12 V to the DC power connector (positive to the central pin): 5 V should be measured on the IC sockets. Diode D4 protects against reverse polarity on the power input. Neither LED should light, but the relay should pull in since sufficient base current should flow through R8 to turn transistor T1 on. In normal operation the base of T1 is taken to ground by the microcontroller, so that the full power supply voltage appears across R8.

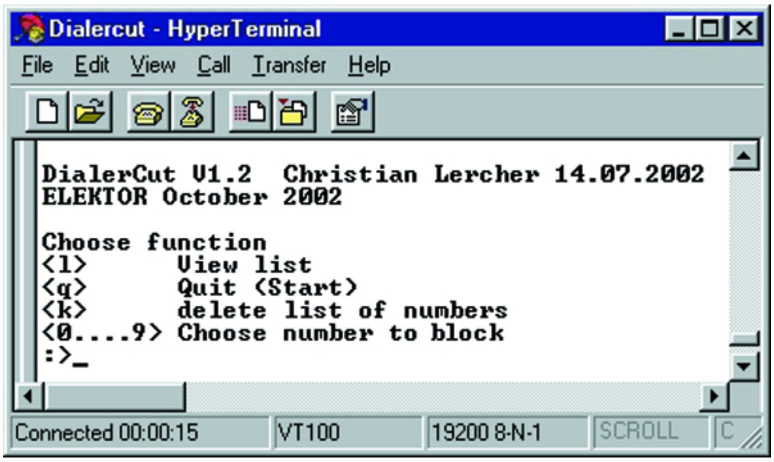
Now disconnect the circuit from the supply and fit the ICs in their sockets. When power is reapplied, relay Re1 should pull in and both LEDs should light until the microcontroller wakes up and all outputs become stable. The current consumption should be around 28 mA.

Disconnect the power again and connect the circuit to a computer using a 9-way RS232 cable (not a null-modem cable). On the PC, run a terminal program (HyperTerminal, for example) with communication settings 19200/8/N/1 and reapply power to the unit. As shown in **Figure 5**, the device is now in configuration mode.

There are only a few commands needed to operate the configuration program:

l list
Gives a list of all barred numbers.

0 to 9 select storage location
Here a series of digits making up a number to be barred can be entered. The character ‘x’ acts as a wildcard, while the ‘enter’ function (or CR) is used to mean ‘disconnect’ as well as terminating the entry.



```
DialerCut V1.2  Christian Lercher 14.07.2002
ELEKTOR October 2002

Choose function
<l>        View list
<q>        Quit (Start)
<k>        delete list of numbers
<0....9>   Choose number to block
:>_
```

Figure 5. HyperTerminal screenshot.

q quit
Switches the unit automatically into active mode, to allow the telephone connection to be tested.

k kill
This function erases the entire contents of the external EEPROM.

Entering the number to be barred proceeds in a straightforward fashion. After a storage location for the number has been selected by pressing a digit from 0 to 9, either a number must be entered or ‘e’ (for ‘exit’) should be pressed. If the ‘enter’ key is pressed immediately, it will be stored in column 0 of the table, and every call will always be dropped immediately. A storage location selected in error should always thus be abandoned using ‘exit’.

Finally we now come to the first test on the telephone network. The unit should be connected to a telephone socket and to a (DTMF-capable) telephone. A normal dial tone should be heard and we can now use the telephone to place a call: after a few moments LED D3 should have lit to indicate that the line is in use. Press a digit key on the telephone, the microcontroller should recognise the digit and LED D3 should go out again.

Assuming this has all worked correctly, replace the receiver, and now try to dial a barred number. The connection should be broken, indicated by the clicking of the relay and the lighting of the red LED.

If this also works correctly, the device is ready for use. Of course, it cannot guarantee one hundred percent safety, since one never knows what methods the hackers will find next to relieve people of their money!

The device works only with analogue systems employing DTMF, and not with older pulse-dialling systems. For ISDN or DSL a completely different digital approach would be required. Of course, the device can be used on the analogue side of an ISDN telephone installation, not just on a modem but also, for example, to bar access to particular extensions.

(020106-1)

Note:
The circuit described in this article is not approved for connection to the public switched telephone network (PSTN) in the UK.

Web links

MT8870, msan-108.pdf:
http://products.zarlink.com
AT24C02:
www.atmel.com/atmel/products/prod162.htm
AT89C2051:
www.atmel.com/atmel/products/prod71.htm
NP-CL-1A81-4/4-218:
www.meder.com/ReedRelays/npcl_se.htm
Telephone connector pinout details:
www.gbnet.net/net/uk-telecom/p3-1.html